

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 1 月 1 5 日
Date of Application:

出 願 番 号 特 願 2 0 0 2 - 3 3 2 5 7 7
Application Number:

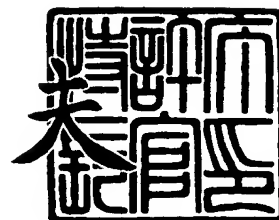
[ST. 10/C] : [J P 2 0 0 2 - 3 3 2 5 7 7]

出 願 人 キヤノン株式会社
Applicant(s):

2 0 0 3 年 1 2 月 2 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康



【書類名】 特許願

【整理番号】 226643

【提出日】 平成14年11月15日

【あて先】 特許庁長官殿

【国際特許分類】 H04N 5/00

【発明の名称】 情報処理装置

【請求項の数】 1

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社
社内

【氏名】 岩村 恵市

【特許出願人】

【識別番号】 000001007

【氏名又は名称】 キヤノン株式会社

【代理人】

【識別番号】 100090273

【弁理士】

【氏名又は名称】 國分 孝悦

【電話番号】 03-3590-8901

【手数料の表示】

【予納台帳番号】 035493

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705348

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置

【特許請求の範囲】

【請求項 1】 所定の作者により作成された原データを処理する情報処理装置であって、

上記原データを変更する際に、その変更に関する変更情報を記憶媒体に記憶する変更情報記憶手段と、

上記変更情報が原本であることを保証するための変更保証情報を作成する変更保証情報作成手段とを有することを特徴とする情報処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置に関し、特に、データの原本性を保証するために用いて好適なものである。

【0002】

【従来の技術】

近年、コンピュータやインターネットの普及に伴い、情報をデジタル化し、デジタルデータとして利用する形態が一般化しつつある。一方、デジタルデータでは、まったく同質なコピーを容易に生成でき、編集処理も容易に実行できるという特徴がある。そのため、デジタルデータの原本性を保証することは重要である。

【0003】

一般に、デジタルデータの原本性を保証するには、米国特許第 5499294 号明細書（特許文献 1）に示されるように、デジタル画像のハッシュ値に公開鍵暗号を用いた電子署名を作成することによって実現できることが知られている。

【0004】

[米国特許第 5499294 号明細書の説明]

上記米国特許第 5499294 号明細書（特許文献 1）に記載されている技術では、電子署名データを生成するために、ハッシュ関数と公開鍵暗号とを使用し

ている。

【0005】

上記電子署名とは、送信者がデータと一緒に該データに対応する署名データを送り、受信者がその署名データを検証して該データの正当性を確認することができるようにするものである。

【0006】

ハッシュ関数と公開鍵暗号とを用いて電子署名データを生成してデータの正当性を確認する方法は、具体的に以下のようになり、これが上記特許文献1に記載されている方法である。

【0007】

まず、秘密鍵を K_s 、公開鍵を K_p とすると、発信者は、平文データ M をハッシュ関数により圧縮して一定長の出力 h を算出する演算を行う。

【0008】

次に、秘密鍵 K_s で一定長の出力 h を変換して電子署名データ s を作成する演算を以下の(1式)により行う。

$$D(K_s, h) = s \cdots (1 \text{ 式})$$

その後、該電子署名データ s と平文データ M とを送信する。

【0009】

一方、受信者は、受信した電子署名データ s を公開鍵 K_p で変換する演算を以下の(2式)により行う。

$$E(K_p, s) = E(K_p, D(K_s, h')) = h' \cdots (2 \text{ 式})$$

【0010】

また、受信者は、受信した平文データ M' を発信者と同じハッシュ関数により圧縮して一定長の出力 h' を算出する演算を行う。そして、この演算で算出された一定長の出力 h' と、上記(2式)により得られた一定長の出力 h' とが一致すれば、受信した平文データ M' が正当であると判断する。

【0011】

平文データ M が送受信間で改ざんされた場合には、上記(2式)により得られた一定長の出力 h' と、受信した平文データ M' を発信者と同じハッシュ関数に

より圧縮して得られた一定長の出力 h' とが一致しないので改ざんを検出できる。

【0012】

ここで、平文データ M の改ざんに合わせて電子署名データ s の改ざんも行われてしまうと改ざんを検出することができなくなる。しかし、電子署名データ s を改ざんするには、一定値の出力 h から平文データ M を求める必要があり、このような計算はハッシュ関数の一方向性により不可能である。

【0013】

次に、ハッシュ関数について説明する。

ハッシュ関数は、上記電子署名データ s の生成を高速化するため等に用いられる。ハッシュ関数は、任意の長さの平文データ M を処理して、一定の長さの出力（一定値の出力） h を出す機能を持つ。ここで、一定値の出力 h を平文データ M のハッシュ値（またはメッセージダイジェスト、デジタル指紋）という。

【0014】

ハッシュ関数に要求される性質として、一方向性と衝突耐性がある。

上記一方向性とは、一定値の出力 h を与えた時に、 $h = H(M)$ となる平文データ M の算出が計算量的に困難であることである。

上記衝突耐性とは、平文データ M を与えた時に、 $H(M) = H(M')$ となる平文データ M' ($M \neq M'$) を算出することが計算量的に困難であること、及び $H(M) = H(M')$ かつ $M \neq M'$ となる平文データ M, M' を算出することが計算量的に困難であることである。

【0015】

ハッシュ関数としては、MD-2、MD-4、MD-5、SHA-1、RIPEMD-128、及びRIPEMD-160等が知られており、これらのアルゴリズムは、一般に公開されている。

【0016】

続いて公開鍵暗号について説明する。

公開鍵暗号は、暗号鍵と復号鍵が異なり、暗号鍵を公開し、復号鍵を秘密に保持する暗号方式である。公開鍵暗号の主な特徴として、以下の3つのことが挙げられる。

(a) 暗号鍵と復号鍵とが異なり暗号鍵を公開できるため、暗号鍵を秘密に配送する必要がなく、鍵配送が容易である。

(b) 各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみを秘密に記憶しておけばよい。

(c) 送られてきた通信文の送信者が偽者でないこと、及びその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。

【 0 0 1 7 】

例えば、平文データ M に対して、公開の暗号鍵 K_p を用いた暗号化操作を $E(K_p, M)$ とし、秘密の復号鍵 K_s を用いた復号化操作を $D(K_s, M)$ とすると、公開鍵暗号アルゴリズムは、次の 2 つの条件を満たす。

【 0 0 1 8 】

(1) 公開の暗号鍵 K_p が与えられたとき、暗号化操作 $E(K_p, M)$ の計算は容易である。秘密の復号鍵 K_s が与えられたとき、復号化操作 $D(K_s, M)$ の計算は容易である。

(2) もし、秘密の復号鍵 K_s を知らないのなら、公開の暗号鍵 K_p と、暗号化操作 E の計算手順と、 $C = E(K_p, M)$ を知っていても、平文データ M を決定することは計算量の点で困難である。

【 0 0 1 9 】

次に、上記 (1)、(2) の条件に加えて、次の (3) の条件が成立することにより、秘密通信を実現できる。

(3) 全ての平文データ M に対し、暗号化操作 $E(K_p, M)$ を定義でき、以下の (4 式) が成立する。

$$D(K_s, E(K_p, M)) = M \cdots (4 \text{ 式})$$

【 0 0 2 0 】

つまり、公開の暗号鍵 K_p は公開されているため、誰もが暗号化操作 $E(K_p, M)$ を計算することができるが、復号化操作 $D(K_s, E(K_p, M))$ を計算して平文データ M を得ることができるのは秘密の復号鍵 K_s を持っている本人だけである。

【 0 0 2 1 】

一方、上記 (1)、(2) の条件に加えて、次の (4) の条件が成立すること

により認証通信を実現できる。

(4) すべての平文データ M に対し、復号化操作 $D(K_s, M)$ を定義でき、以下の (5 式) が成立する。

$$E(K_p, D(K_s, M)) = M \cdots (5 \text{ 式})$$

【0 0 2 2】

つまり、復号化操作 $D(K_s, M)$ を計算できるのは、秘密の復号鍵 K_s を持っている本人のみであり、他の人が偽の秘密の復号鍵 K_s' を用いて復号化操作 $D(K_s', M)$ を計算し、秘密の復号鍵 K_s を持っている本人になりすましたとしても、上記 (5 式) が成立しないので $(E(K_p, D(K_s', M))) \neq M$ 、受信者は、受けとった情報が不正なものであることを確認できる。

【0 0 2 3】

また、復号化操作 $D(K_s, M)$ が改ざんされても上記 (5 式) が成立しなくなり $(E(K_p, D(K_s, M)')) \neq M$ 、受信者は、受けとった情報が不正なものであることを確認できる。

【0 0 2 4】

上記の秘密通信と認証通信とを行うことができる代表例として、RSA暗号やR暗号やW暗号等が知られている。

ここで、現在最も使用されている上記RSA暗号による暗号化と復号は、以下の (6 式) で示される。

【0 0 2 5】

暗号化：暗号化鍵 (e, n) 暗号化変換 $C = M^e \pmod{n}$

復号：復号鍵 (d, n) 復号変換 $M = C^d \pmod{n}$

$$n = p \cdot q$$

ここで、 p 、 q は、大きな異なる素数 \cdots (6 式)

【0 0 2 6】

【特許文献 1】

米国特許第 5 4 9 9 2 9 4 号明細書

【0 0 2 7】

【発明が解決しようとする課題】

しかしながら、米国特許第 5 4 9 9 2 9 4 号明細書に記載されている手法では、電子署名をつけたデジタルデータを 1 ビットでも変更した場合、著者が認めた正当な変更であっても、改ざんとして検出される。

【 0 0 2 8 】

さらに、米国特許第 5 4 9 9 2 9 4 号明細書に記載されている手法では、データを変更した後に關しては、その変更したデータが原本でないことだけが分かるだけである。

【 0 0 2 9 】

例えば、米国特許第 5 4 9 9 2 9 4 号明細書をデジタルカメラに適用した例を考える。通常、デジタルカメラからの出力であるデジタル画像と電子署名データは、コンピュータ (PC) に取り込まれる。

【 0 0 3 0 】

その後、画像が見やすいように輝度を変更したり、フィルタリングをしたり、または画像を小さくするために余計な部分を切り取ったりすることは通常よく行われる。

【 0 0 3 1 】

これらの処理は、画像を見やすく、分かりやすくするための処理であり、デジタル画像の著作者が認めている処理である場合が多い。しかしながら、米国特許第 5 4 9 9 2 9 4 号明細書に記載されている技術では、デジタルカメラから出力された後に行われた全ての処理は改ざんとして検出される。

【 0 0 3 2 】

このように従来の技術では、電子署名などによりデータの原本性が保証されているような場合には、上記データを正当なデータとして変更することができないという問題点があった。

【 0 0 3 3 】

本発明は上述の問題点に鑑みてなされたものであり、データの原本性を保証しながら、上記データの作者が認める正当な変更を行えるようにすることを目的とする。

【 0 0 3 4 】

【課題を解決するための手段】

本発明の情報処理装置は、所定の作者により作成された原データを処理する情報処理装置であって、上記原データを変更する際に、その変更に関する変更情報を記憶媒体に記憶する変更情報記憶手段と、上記変更情報が原本であることを保証するための変更保証情報を作成する変更保証情報作成手段とを有することを特徴としている。

【0035】**【発明の実施の形態】****(第1の実施の形態)**

次に、本発明の情報処理装置の第1の実施の形態を、図面を参照しながら説明する。なお、ここではオリジナルのデジタルデータを原画像と呼ぶが、本実施の形態で適用されるデジタルデータ（原データ）は、デジタル画像だけに限らず、デジタルデータ全てに適用できる。

【0036】

まず、原画像に対する電子署名を生成する。これは、前述した米国特許第5499294号明細書のように、原画像に対するハッシュ値を生成し、それに対して秘密鍵で電子署名を作成することによって実現できる。この電子署名を第1の署名（図1の署名0）11と表し、図1（a）に示されるように原画像12とともに保存する。

【0037】

次に、保存された原画像12に対して第1の処理を施して、その処理結果を正当な画像として認める場合を考える。上述した米国特許第5499294号明細書に記載されている電子署名の原理は、デジタルデータ全てに使える公知の技術である。したがって、上述した米国特許第5499294号明細書に記載されている電子署名の原理を用いて、履歴情報13に対する電子署名を作成する。ここで、履歴情報13とは、上記第1の処理で行われた原画像12の変更（履歴）に関する情報である。なお、以下の説明では、この履歴情報13に対する電子署名を第2の署名（図1の署名1）14と称する。

【0038】

例えば、上記第 1 の処理が、フォトショップ ver.X というエディタで行った輝度変換である場合、上記第 1 の処理に対する履歴情報 1 3 は、対象画像を特定する情報と、エディタを特定する情報と、上記エディタで規定されている輝度変換というフィルタ名と、それに用いたパラメータ情報などから構成される。

【 0 0 3 9 】

また、履歴情報 1 3 は、原画像 1 2 と変更画像との差分データを含んでいても良い。ここで、対象画像を特定する情報は、原画像 1 2 の ID 番号や、原画像 1 2 の署名である第 1 の署名（図 1 の署名 0）などを用いることができる。ただし、履歴情報 1 3 が長い場合には、ハッシュ値を生成し、それに署名してもよい。そして、このようにして作成された履歴情報 1 3 と第 2 の署名 1 4 を図 1（b）に示されるように原画像 1 2 と一緒に保存する。

【 0 0 4 0 】

上記の処理は、著作者によって行われる処理である。次に、上記第 1 の処理により輝度変換された画像の入手を他のユーザが希望している場合を考える。著作者は、図 1（b）のように、記憶媒体に保存されている原画像 1 2、第 1 の署名（図 1 の署名 0）1 1、履歴情報 1 3、及び第 2 の署名（図 1 の署名 1）1 4 を、通信手段を用いてそのユーザに送信する。以下、これらの情報が送られたユーザが行う検証処理について説明する。

【 0 0 4 1 】

まず、原画像 1 2 に対する第 1 の署名（図 1 の署名 0）1 1を確認する。この処理は、前記の米国特許第 5 4 9 9 2 9 4 号明細書において説明した検証処理と同じ手法によって実現できる。次に、履歴情報 1 3 に対する第 2 の署名（図 1 の署名 1）を確認する。これも電子署名の確認手順（上記検証処理）により実現できる。

【 0 0 4 2 】

この 2 つのデータの正当性が電子署名により確認された後、履歴情報 1 3 に書かれた上記第 1 の処理と同じ処理を、原画像 1 2 に対して行うことにより、ユーザは、輝度変換された画像を得ることができる。

【 0 0 4 3 】

図4は、以上のような処理を行う本実施形態の情報処理装置の構成の一例を示したブロック図である。なお、本発明の情報処理装置の実現に当たっては、図3に示される全ての機能を使用することは必須ではない。

【0044】

図4において、情報処理装置（コンピュータ）301のハードウェアは、一般に普及しているパーソナルコンピュータであり、スキャナ等の画像入力装置317から読み取られた画像を入力し、編集や保管を行うことが可能である。

【0045】

また、画像入力装置317で得られた画像をプリンタ316から印刷させることができる。なお、ユーザからの各種指示等は、マウス313やキーボード314などからの入力操作により行われる。

【0046】

コンピュータ301の内部では、バス307により後述する各ブロックが接続され、種々のデータの受け渡しが可能である。図3において、MPU302は、コンピュータ301内部の各ブロックの動作を制御し、あるいは内部に記憶されたプログラムを実行することができる。

【0047】

主記憶装置303は、MPU302において行われる処理のために、一時的にプログラムや処理対象の画像データを格納しておく装置である。ハードディスク（HDD）304は、主記憶装置303等に転送されるプログラムや画像データをあらかじめ格納したり、処理後の画像データを保存したりすることのできる装置である。

【0048】

スキャナインタフェース（I/F）315は、原稿やフィルム等を読み取って、画像データを生成するスキャナ317と接続され、スキャナ317で得られた画像データを入力することのできるインターフェース（I/F）である。

【0049】

プリンタインタフェース308は、画像データを印刷するプリンタ316と接続され、印刷する画像データをプリンタ316に送信することのできるインター

フェース（I／F）である。

【0050】

CDドライブ（CD）309は、外部記憶媒体の一つであるCD（CD-R／CD-RW）に記憶されたデータを読み出したり、あるいは書き込んだりすることができる装置である。

【0051】

FDDドライブ（FDD）311は、CDドライブ309と同様に、外部記憶装置の一つであるFDDからの読み出しや、FDDへの書き込みをすることができる装置である。

【0052】

DVDドライブ（DVD）310は、FDDドライブ311と同様に、外部記憶装置の一つであるDVDからの読み出しや、DVDへの書き込みをすることができる装置である。

【0053】

なお、CD、FDD、DVD等に画像編集用のプログラム、あるいはプリンタドライバが記憶されている場合には、これらプログラムをハードディスク（HDD）304上にインストールし、必要に応じて主記憶装置303に転送されるようになっている。

【0054】

インターフェース（I／F）312は、マウス313やキーボード314からの入力指示を受け付けるために、これらと接続されるインターフェース（I／F）である。

【0055】

また、モニタ306は、透かし情報の抽出処理結果や処理過程を表示することのできる表示装置である。さらに、ビデオコントローラ305は、表示データをモニタ306に送信するための装置である。

【0056】

なお、本実施の形態では、情報処理装置301に上述した機能を全て搭載するようにしたが、上述した機能を分配して複数の装置からなるシステムとしてもよ

い。すなわち、複数の機器（例えば、ホストコンピュータ、インターフェース機器、リーダ、プリンタ等）から構成されるシステムにしても、一つの機器からなる装置（例えば、複写機、ファクシミリ装置等）にしてもよい。

【0057】

次に、図2と図3を参照しながら、本実施の形態の情報処理装置301の動作について説明する。図2は、電子署名を生成する際の情報処理装置301の処理を説明するフローチャートである。また、図3は、電子署名を検証する際の情報処理装置301の処理を説明するフローチャートである。

【0058】

なお、原画像12に対する第1の署名（図1の署名0）を生成する際の処理は、上述した米国特許第5499294号明細書に記載されている技術と同様にして行えるので説明を省略し、ここでは、原画像12と第1の署名（図1の署名0）11が、情報処理装置301内の記憶媒体に保存されているという前提で説明する。

【0059】

まず、図2に示す電子署名（第2の署名（図1の署名1）14）を生成する際の処理を説明する。なお、以下では必要に応じてこの処理を署名生成処理と称する。

記憶媒体に保存された原画像12を入力する（ステップS201）。これは、ハードディスク（HDD）304、CDドライブ（CD）309、DVDドライブ（DVD）310、またはFDDドライブ（FDD）311などに接続された各記憶媒体に格納されている原画像12を、マウス313やキーボード314からの入力指示により、主記憶装置303にロードすることにより実現される。

【0060】

次に、その原画像12に対して変更処理を行う（ステップS202）。このときに行った変更処理に関する履歴情報13（上記記対象画像特定情報や、エディタ特定情報、処理を特定するフィルタリング名やそのパラメータなど）を記憶媒体に記憶する（ステップS203）。

【0061】

なお、この変更処理は、複数の処理を組み合わせても良い。また、変更処理を行った結果、変更処理した画像が正当であると認められない場合には、処理結果及び処理履歴を廃棄し、前の画像（原画像 1 2）に戻すこともできる。

【 0 0 6 2 】

そして、これらの処理は、マウス 3 1 3 やキーボード 3 1 4 からの入力指示に応じて主記憶装置 3 0 3 にロードしたプログラムを、MPU 3 0 2 などを用いて実行することにより行われる。このとき、モニタ 3 0 6 により実行状況や、その結果をモニタすることも可能である。

【 0 0 6 3 】

次に、その処理結果を正当な画像として認める場合（ステップ S 2 0 4）、記憶媒体に記憶された履歴情報 1 3 に対して電子署名（第 2 の署名（図 1 の署名 1） 1 4）を作成する（ステップ S 2 0 5）。これらの処理も、マウス 3 1 3 やキーボード 3 1 4 からの入力指示に応じて主記憶装置 3 0 3 にロードしたプログラムを、MPU 3 0 2 などを用いて実行することにより行われる。

【 0 0 6 4 】

最後に、生成した原画像 1 2、第 1 の署名（図 1 の署名 0） 1 1、履歴情報 1 3、及び第 2 の署名（図 1 の署名 1） 1 4 を、ハードディスク 3 0 4、CD ドライブ 3 0 9、DVD ドライブ 3 1 0、または FDD ドライブ 3 1 1 などに保存する（ステップ S 2 0 6）。

【 0 0 6 5 】

次に、図 3 に示す電子署名を検証する際の処理を説明する。なお、以下では、必要に応じてこの処理を署名検証処理と称する。

なお、電子署名（第 1 の署名 1 1 及び第 2 の署名 1 4）の検証処理を行うときには、第 1 の署名（図 1 の署名 0） 1 1、履歴情報 1 3、及び第 2 の署名（図 1 の署名 1） 1 4 を、情報処理装置 3 0 1 が持っていることを前提とする。ただし、以下の処理も、図 4 に示す情報処理装置 3 0 1、特に、マウス 3 1 3 やキーボード 3 1 4 からの入力指示により主記憶装置 3 0 3 にロードしたプログラムを、MPU 3 0 2 などを用いて実行することにより行われる。

【 0 0 6 6 】

まず、原画像 1 2 に対する第 1 の署名（図 1 の署名 0） 1 1 を確認する（ステップ S 2 1 1）。次に、履歴情報 1 3 に対する第 2 の署名（図 1 の署名 1） 1 4 を確認する（ステップ S 2 1 2）。

【 0 0 6 7 】

次に、この 2 つのデータ（原画像 1 2 と履歴情報 1 3）の正当性が、電子署名（第 1 の署名 1 1 と第 2 の署名 1 4）により確認された場合には（ステップ S 2 1 3）、履歴情報 1 3 に書かれている処理と同じ処理を原画像 1 2 に対して行う。これにより、ユーザは、輝度変換された画像を得る（ステップ S 2 1 4）。

【 0 0 6 8 】

一方、ステップ S 2 1 3 において、署名が正しくないと判定された場合には、原画像 1 2 及び履歴情報 1 3 のうちの少なくとも何れか一方は正しくないので処理を中止する。また、このように署名が正しくない場合には、情報（原画像 1 2、履歴情報 1 3）に改ざんがあることをユーザに通知するようにしてもよい。

【 0 0 6 9 】

以上のように、本実施の形態では、原画像 1 2 に対する第 1 の署名（図 1 の署名 0） 1 1 を保持するようにしたので、原画像 1 2 に対する原本性を保証できる。

そして、履歴情報 1 3 に対する第 2 の署名（図 1 の署名 1） 1 4 を保持するようにしたので、原画像 1 2 の変更処理に対する正当性を保証できる。したがって、原画像 1 2 に対して、著作者が認める正当な変更を行うことができ、画像の最新性を保証できる。

【 0 0 7 0 】

ところで、上述したように、米国特許第 5 4 9 9 2 9 4 号明細書に記載されている技術では、例えば、デジタルカメラから出力された後に行われた全ての処理は改ざんとして検出される。

【 0 0 7 1 】

そこで、著者が自分の署名用の秘密鍵を用いて、変更を認めた変更画像に対して電子署名をつけるという解決策が考えられる。しかしながら、この場合、署名した変更画像は独立した画像となり、原画像 1 2 と、原画像 1 2 を変更すること

により得られる変更画像との関係が分からなくなるという問題点が残る。さらに、いくつかの変更を著者が正当と認めた場合、多くの画像と署名のペアを管理する必要がある、メモリの制約もでてくる可能性がある。

【0072】

これに対して本実施の形態では、第1の署名（図1の署名0）11及び第2の署名（図1の第2の署名1）14が正しければ、原画像12と変更画像との間の関係（処理履歴）を履歴情報13により知ることができる。

【0073】

さらに、履歴情報13は、変更画像に比べてデータ量が少ないので、多くの履歴情報13を保存しても、それに対応する変更画像をすべて保存することに比べてメモリ容量が小さくなる。これは、後述する第2の実施の形態に示す複数回の変更処理に対して特に有効である。

【0074】

また、履歴情報13と署名情報（第1の署名11、第2の署名14）は、画像情報に比べて小さいので、原画像12のヘッダなどに格納することが容易で、多くの履歴情報13があっても1つのファイルとして管理できる。これも後述する第2の実施の形態に示す複数回の変更処理に対して特に有効である。

【0075】

（第2の実施の形態）

次に、本発明の第2の実施の形態を説明する。なお、本実施の形態の説明において、上述した第1の実施の形態と同一の部分については同一の符号を付して詳細な説明を省略する。

【0076】

上述した第1の実施の形態では、1回の処理に対する例を示したが、本実施の形態では、第1の処理の後に、第2の処理、第3の処理・・・と続けてそれらを正当な処理として認められるようにしている。すなわち、本実施の形態では、以下に示すようにして、原画像12の原本性を保証しながら、複数回の変更処理による画像の最新性を保証できるようにしている。

【0077】

例えば、第1の実施の形態の情報処理装置301で生成した履歴情報13を第1の履歴（図5の履歴1）と表す。第1の実施の形態では、図2のフローチャートに従って行われる処理の前提として、原画像12と第1の署名（署名0）11は保存されているとしたが、本実施の形態では、2回目の変更に対しては第1の履歴（図5の履歴1）13と、それに対する第2の署名（署名1）14も保存されているとして、図2のフローチャートに従った処理を行う。

【0078】

その結果、2回目の変更に対する履歴情報として第2の履歴（図5の履歴2）15と、この第2の履歴15に対する電子署名である第3の署名（図5の署名2）16とが生成される。その結果、原画像12、第1の署名（署名0）11、第1の履歴（履歴1）13、及び第2の署名（署名1）14に加えて、第3の履歴（図5の履歴2）15と第2の署名（図5の署名2）16とが保存される。

【0079】

以下同様にして変更処理を繰り返せば、N（Nは自然数）回の変更処理に対して、原画像12と、第1～第Nの履歴（図5の履歴1～履歴N）と、第1～第（N+1）の署名（図5の署名0～署名N）とが署名生成処理によって生成され、保存されることになる（図5（a）を参照）。

【0080】

一方、この署名生成処理に対する署名検証処理では、図3のフローチャートにおけるステップS211の処理、すなわち原画像12に対する署名確認の処理を行った後に、ステップS212において、第2の署名（署名1）13の検証だけでなく、第3～第N+1の署名（図5の署名2～署名N）（についても検証を行う。そして、ステップS213において、これら第2～第（N+1）の署名（図5の署名1～署名N）が正しいと判断された場合には、ステップS214において、原画像12に対し、第1～第Nの履歴（図5の履歴1～履歴N）の処理を実行し、原画像12を変更する。

【0081】

なお、この場合において、第2～第M（Mは、（N+1）より小さい自然数）の署名までは正しく、それ以降の署名が正しくない場合には、全ての処理を中止

しなくても第 2 ～ 第 M の署名に対する処理を行い、それ以降の署名に対する処理を中止することもできる。

【 0 0 8 2 】

以上のように本実施の形態では、1 ～ N 回目の変更に対する履歴情報である第 1 ～ 第 N の履歴と、この第 1 ～ 第 N の履歴に対する電子署名である第 2 ～ 第 (N + 1) の署名とを生成するようにし、第 1 ～ 第 N の履歴が正しいかどうかを、第 2 ～ 第 (N + 1) の署名を用いて判断し、正しい場合には第 1 ～ 第 N の履歴に従って原画像 1 2 を変更するようにしたので、1 回の変更だけでなく、著作者が正当と認めれば複数回の変更処理を追加しても画像の最新性を常に保証できる。

【 0 0 8 3 】

なお、著作者が、第 1 の処理を含まない新たな第 2 の処理も正当と認める場合には、第 1 の処理の代わりに第 2 の処理の履歴情報に対して図 2 と図 3 に示したフローチャートに従った処理を行えば、第 2 の処理に対する変更の正当性と原本性とが第 1 の実施の形態と同様にして保証できることは明らかである。この場合、第 1 の処理と第 2 の処理に関する関係は、図 5 (b) のようになる。このとき、図 6 に示すようなリスト 6 0 に、履歴情報と電子署名とを処理ごとにまとめて別管理したり、履歴情報のなかにその処理の目的・効果などのアブストラク的な情報を入れておいたりすることもできる。

【 0 0 8 4 】

(第 3 の実施の形態)

次に、本発明の第 3 の実施の形態を説明する。なお、本実施の形態の説明において、上述した第 1 及び第 2 の実施の形態と同一の部分については同一の符号を付して詳細な説明を省略する。

【 0 0 8 5 】

上述した第 1 及び第 2 の実施の形態では、処理の変更はすべて著作者が行う例を示したが、本実施の形態では、多くのユーザが 1 つのデジタルデータを変更することができるようにする。ここでは、デジタルデータとして電子文書を想定する。

【 0 0 8 6 】

そして、図 7 に示すように、複数のユーザ 6 0 3 ～ 6 0 5 がサーバ 6 0 1 上で共有している電子文書 6 0 2 を、ネットワーク 6 0 0 を介して各ユーザ 6 0 3 ～ 6 0 5 が取り込んで完成させる場合を想定する。

【 0 0 8 7 】

なお、上記においてユーザ 6 0 3 ～ 6 0 5 とは、ユーザが所有する端末のことであり、この端末のハードウェアは、例えば図 4 に示した情報処理装置 3 0 1 により構成されるものである。以下、サーバ 6 0 1 及びユーザ 6 0 3 ～ 6 0 5 における処理の内容について説明する。

【 0 0 8 8 】

まず、ユーザ 6 0 3 が最初のたたき台となる電子文書 6 0 2 を作成し、作成した電子文書 6 0 2 を第 1 の文書として、それに対する署名をつけてサーバ 6 0 1 に保存する。なお、以下の説明では、第 1 の文書に対する署名を第 1 の署名と称する。また、この第 1 の署名は、上述した第 1 及び第 2 の実施の形態で説明した第 1 の署名（署名 0） 1 1 と同じ方法で作成される。

【 0 0 8 9 】

次に、サーバ 6 0 1 に保存された電子文書 6 0 2 をユーザ 6 0 4 が修正したい場合、ユーザ 6 0 4 は、まず、第 1 の文書とそれに対する第 1 の署名を確認する。それが正当であれば、第 1 の文書に対して修正を施して第 2 の文書を作成し、その修正に関する履歴情報と、この履歴情報に対する署名を付加して保存する。

【 0 0 9 0 】

なお、以下の説明では、この第 1 の文書の修正に関する履歴情報を第 1 の履歴情報と称する。また、第 1 の履歴情報に対する署名を第 2 の署名と称する。そして、これら第 1 の履歴情報と第 2 の署名は、それぞれ上述した第 1 及び第 2 の実施の形態で説明した第 1 の履歴情報（履歴 1） 1 3 と第 2 の署名（署名 1） 1 4 と同じ方法で作成される。

【 0 0 9 1 】

次に、ユーザ 6 0 5 が修正したい場合、ユーザ 6 0 5 は、それまでの署名（第 1 の署名と第 2 の署名）を確認し、それらが正当であれば、第 2 の文書の修正を施して第 3 の文書を生成し、その修正に関する履歴情報と、この履歴情報に対す

る署名を付加して保存する。

【0092】

なお、以下の説明では、第2の文書の修正に関する履歴情報を第2の履歴情報と称する。また、第2の履歴情報に対する署名を第3の署名と称する。また、これら第2の履歴情報と第3の署名は、それぞれ上述した第1及び第2の実施の形態で説明した第2の履歴情報（履歴2）15と第3の署名（署名2）16と同じ方法で作成される。

【0093】

以下、他のユーザまたは同じユーザが文書の修正を繰り返したい場合、修正に関する履歴情報と、この履歴情報に対する署名を付加していくことにより、複数のユーザによる電子文書の管理を実現することができる。

【0094】

ただし、あるユーザが、それまでの署名を確認したときに、署名が正当でなければその旨を他のユーザに通知する。また、あるユーザが、第1～第M（Mは自然数）の履歴情報までの修正は良いと思うが、それ以降の修正は良くないと思う場合には、良いと思う履歴情報までの修正を行った第Mの文書を作成し、そのあと第（M+1）の履歴情報とは異なる修正を行う。その後、第Mの文書を対象文書として特定する情報（文書番号やハッシュ値など）を履歴情報に入れて、その署名を作成することもできる。この場合、第2の実施の形態で説明した図5（b）のように、作成した署名がそれまでの署名と並列の関係になるので、文書管理システムの中に図6のような署名の関係を示すリスト60を作成し、分かりやすくすることも可能である。

【0095】

（第4の実施の形態）

次に、本発明の第4の実施の形態を説明する。なお、本実施の形態の説明において、上述した第1～第3の実施の形態と同一の部分については同一の符号を付して詳細な説明を省略する。

【0096】

本実施の形態では、医療画像に対する医療画像管理システムを例にとり説明す

る。

システムとしては、図 7 と同様に、複数のユーザ（医者） 6 0 3 ～ 6 0 5 がデジタルレントゲン画像などの電子化された医療画像 6 0 2 をネットワーク 6 0 0 で接続されたサーバ 6 0 1 上に共有している場合を想定する。

【 0 0 9 7 】

この場合、医療画像 6 0 2 に対する原本性を保証するための情報である第 1 の署名は、デジタルレントゲン機器に保存されているか、またはデジタルレントゲン機器における医療画像 6 0 2 の出力時点で生成され、サーバ 6 0 1 に保存されているとする。

【 0 0 9 8 】

まず、医者 6 0 3 が医療画像 6 0 2 を見る場合、画像内容に関する編集は行わないが輝度変換などの視覚的效果に関する変更を行う。このとき、医者 6 0 3 は、毎回その輝度変更を行わないようにするために、原画像である医療画像 6 0 2 と変更画像との差分をとり、対象画像を特定する情報や上述したその変更に関するアブストラク的な情報を、医療画像 6 0 2 に付加して第 1 の履歴情報として保存する。

【 0 0 9 9 】

そして、この第 1 の履歴情報のハッシュ値に自分の署名を生成し、第 2 の署名としてサーバ 6 0 1 に保存するか、または自分（医者 6 0 3）が所有する端末に保存する。なお、これら第 1 の履歴情報と第 2 の署名は、それぞれ上述した第 1 ～第 3 の実施の形態で説明した第 1 の履歴情報（履歴 1） 1 3 と第 2 の署名（署名 1） 1 4 と同じ方法で作成される。

【 0 1 0 0 】

次に、医者 6 0 4 が医療画像 6 0 2 を見る場合、その原本性を第 1 の署名により確認し、他の医者 6 0 3 の処理を確認するために第 1 の履歴情報の正当性を第 2 の署名により確認し、それを利用またはさらに処理を追加する。

【 0 1 0 1 】

ここで、処理を追加する場合は、第 1 の履歴情報に従った変更が施された医療画像を変更対象とする場合には、変更対象とする画像に対する情報として第 2 の

署名を第2の履歴情報に含め、さらに、変更対象とする画像と、自分が作成した変更画像との差分画像などを加えて、第3の署名を生成する。また、原画像（医療画像602）を変更対象とする場合、第1の署名を第2の履歴情報に含め、さらに、原画像（医療画像602）と、自分が作成した変更画像との差分画像などを加えて、第3の署名を生成する。

【0102】

以下、同様の処理を行うことにより、本実施の形態の医療画像管理システムにおいて、原画像の原本性と変更処理の正当性、及び画像の最新性を同時に実現できる。なお、上記において、第2の履歴情報と第3の署名は、それぞれ上述した第1～第3の実施の形態で説明した第2の履歴情報（履歴2）15と第3の署名（署名2）16と同じ方法で作成される。

【0103】

（第5の実施の形態）

次に、本発明の第5の実施の形態を説明する。なお、本実施の形態の説明において、上述した第1～第4の実施の形態と同一の部分については同一の符号を付して詳細な説明を省略する。

【0104】

本実施の形態では、著作物管理システムを用いたビジネスモデルに関する説明を行う。

ここでは、ネットワークに複数のユーザと原画像に対し1次著作権を保有する著作権者がある場合を考える。よって、著作権者は、図1（a）のように、原画像12とそれに対する第1の署名（署名0）11を有しているとする。

【0105】

図8のフローチャートを参照しながら、本実施の形態のシステムにおける処理を説明する。

まず、著作権者は、課金などにより正当と認められたユーザに対して、原画像12を配布する（ステップS701）。ただし、この原画像12には、電子透かしなどの著作権保護のための仕組みが入っていても良い。また、この原画像12には、上述した原本性を示す第1の署名（署名0）11も添付され配布される。配

布された原画像 12 については、ユーザの利用範囲内で変更することが認められているが、原画像 12 を含むその変更画像の配布は認められていないとする。

【0106】

ユーザは、各々、原画像 12 の署名を確認した後、著作者から配布された原画像 12 に対して、いくつかの変更を試みる（ステップ S702）。ユーザが面白いと思った変更画像を正当な 2 次著作物としたい場合、ユーザは、著作者に、原画像 12 と第 1 の署名（署名 0）11 に加えて自ら行った変更に関する履歴情報である第 1 の履歴情報 13 とその電子署名である第 2 の署名（署名 1）14 を著作者に送る（ステップ S703）。ただし、第 2 の署名（署名 1）14 は、ユーザの秘密鍵で署名されており、それを確認する公開鍵も一緒に送付することができる。

【0107】

著作者は、第 1 の署名（署名 0）11 と、第 2 の署名（署名 1）14 を確認し、原画像 12 に対して第 1 の履歴情報 13 に応じた処理を施す（ステップ S704）。著作者がその処理結果を判定して（ステップ S705）、2 次著作物として許諾する場合には、第 1 の履歴情報 13 に対して著作者の鍵による電子署名を生成し、原画像 12 と第 1 の署名（署名 0）11 と、第 1 の履歴情報 13 と、第 2 の署名（署名 1）14 と、第 3 の署名（署名 2）16 とを一緒に保存する（ステップ S706）。一方、許諾しない場合は第 3 の署名（署名 2）16 を生成せずに、その旨をユーザに通知する。

【0108】

これにより、著作者は、原画像 12 である 1 次著作物から効率的に 2 次著作物を生成する仕組みを実現することができ、各ユーザは、自分が生成した 2 次著作物を正当に認められる仕組みを実現することができる。このとき、著作者は複数の 2 次著作物からの著作権料を得ることができ、各ユーザは 1 次著作物を基に容易に 2 次著作物を生成でき、それによる 2 次著作権料も得ることができる。さらに、3 次著作物以降に対しても全く同様にして適用できる。

【0109】

（その他の実施の形態）

本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記録媒体（または記憶媒体）を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはCPUやMPU）が記録媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。この場合、記録媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記録した記録媒体は本発明を構成することになる。

【0 1 1 0】

また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム（OS）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0 1 1 1】

さらに、記録媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0 1 1 2】

本発明を上記記録媒体に適用する場合、その記録媒体には、先に説明したフローチャートに対応するプログラムコードが格納されることになる。

【0 1 1 3】

本発明の実施態様の例を以下に列挙する。

（実施態様1） 所定の作者により作成された原データを処理する情報処理装置であって、上記原データを変更する際に、その変更に関する変更情報を記憶媒体に記憶する変更情報記憶手段と、上記変更情報が原本であることを保証するための変更保証情報を作成する変更保証情報作成手段とを有することを特徴とする

情報処理装置。

【0 1 1 4】

(実施態様 2) 上記原データが原本であることを保証するための原データ保証情報を作成する原データ保証情報作成手段をさらに有することを特徴とする実施態様 1 に記載の情報処理装置。

【0 1 1 5】

(実施態様 3) 上記原データを変更することが指示された際に、上記指示された内容に従って上記原データを変更する処理を行うための変更処理手段をさらに有することを特徴とする実施態様 1 または 2 に記載の情報処理装置。

【0 1 1 6】

(実施態様 4) 上記変更保証情報と、上記原データ保証情報は、デジタル署名であることを特徴とする実施態様 1 ～ 3 の何れか 1 項に記載の情報処理装置。

【0 1 1 7】

(実施態様 5) 上記変更情報は、上記原データを特定する情報と、上記変更処理手段を特定する情報と、上記原データを変更する際に行った変換処理を特定する情報とを含むことを特徴とする実施態様 1 ～ 4 の何れか 1 項に記載の情報処理装置。

【0 1 1 8】

(実施態様 6) 上記変更情報は、上記原データと、上記原データに対する変更データとの差分情報を含むことを特徴とする実施態様 1 ～ 5 の何れか 1 項に記載の情報処理装置。

【0 1 1 9】

(実施態様 7) 上記原データと、上記原データ保証情報と、上記変更情報と、上記変更保証情報とを一体として管理する管理手段をさらに有することを特徴とする実施態様 1 ～ 6 の何れか 1 項に記載の情報処理装置。

【0 1 2 0】

(実施態様 8) 上記原データと、上記原データ保証情報と、上記変更情報と、上記変更保証情報とを一体として送付する送付手段をさらに有することを特徴とする実施態様 1 ～ 7 の何れか 1 項に記載の情報処理装置。

【0 1 2 1】

(実施態様 9) 所定の作者により作成された原データを処理する情報処理装置であって、上記原データが正当なものであることを確認する原データ確認手段と、上記原データの変更にに関する変更情報が正当なものであることを確認する変更情報確認手段と、上記原データと上記変更情報が正当であることが確認された場合に、上記変更情報に応じて上記原データを変更する原データ変更手段とを有することを特徴とする情報処理装置。

【0 1 2 2】

(実施態様 1 0) 上記原データ確認手段は、上記原データに対するデジタル署名を検証し、上記変更情報確認手段は、上記変更情報に対するデジタル署名を検証するようにしたことを特徴とする実施態様 9 に記載の情報処理装置。

【0 1 2 3】

(実施態様 1 1) 所定の作者により作成された原データを処理する情報処理装置であって、上記原データの変更にに関する変更情報と、上記原データの変更履歴とを管理する管理手段を有することを特徴とする情報処理装置。

【0 1 2 4】

(実施態様 1 2) ネットワークに接続された上記実施態様 1 ～ 1 1 の何れか 1 項に記載の情報処理装置を複数有し、上記複数の情報処理装置は、上記ネットワーク上で共有された電子データが正当なものであることと、上記電子データの変更にに関する第 1 の変更情報が正当なものであることを確認する確認手段と、上記電子データと、上記第 1 の変更情報とが、上記確認手段により正当なものであることが確認された場合に、上記電子データを変更する電子データ変更手段と、上記電子データ変更手段により変更された電子データの変更にに関する第 2 の変更情報と、上記第 2 の変更情報が正当なものであることを保証するための変更保証情報とを作成する情報作成手段と、上記情報作成手段により作成された第 2 の変更情報と、変更保証情報とを上記ネットワークに送信する送信手段とを有し、上記複数の情報処理装置で共同して上記電子データの作成と管理を行うようにしたことを特徴とする電子データ管理システム。

【0 1 2 5】

(実施態様 13) 上記第 1 及び第 2 の変更情報と、上記原データの変更履歴を表す情報とのうち、少なくとも何れか一方を管理する変更履歴管理手段を有し、上記変更履歴管理手段を利用して上記複数の情報処理装置で共同して上記電子データを作成することを特徴とする実施態様 12 に記載の電子データ管理システム。

【0126】

(実施態様 14) 上記複数の情報処理装置は、上記電子データ及び上記第 1 の変更情報のうち少なくとも何れか一方が正当でないということが上記確認手段により確認された場合に、その旨を他の情報処理装置に通知する通知手段をさらに有することを特徴とする実施態様 12 または 13 に記載の電子データ管理システム。

【0127】

(実施態様 15) 1 次著作物の著作者が所有する第 1 の情報処理装置と、上記第 1 の情報処理装置とネットワークを介して接続された第 2 ～第 n の情報処理装置とを有し、上記第 2 ～第 n の情報処理装置のうち、上記著作者が正当と認めたユーザが所有する情報処理装置に対して、上記第 1 の情報処理装置から上記 1 次著作物を配布する 1 次著作物配布手段と、上記 1 次著作物配布手段により 1 次著作物が配布された情報処理装置により、上記著作者から認められた許諾範囲内で 1 次著作物を変更し、その変更内容を表す変更情報と、その変更情報が原本であることを保証するための第 1 の変更保証情報とを、上記第 1 の情報処理装置に送信する送信手段と、上記変更情報と上記第 1 の変更保証情報との送信先である上記第 1 の情報処理装置により、上記送信された変更情報が正当なものであることを、上記第 1 の変更保証情報を用いて確認し、正当であることを確認した場合に、上記送信された変更情報が正当なものであることを保証するための第 2 の変更保証情報を上記変更情報に付加して送信元の情報処理装置に返信する返信手段とを有し、上記変更情報と、上記第 2 の変更保証情報とが返信された情報処理装置に対して、上記 1 次著作物を変更したものを 2 次著作物として使用することを許諾するようにしたことを特徴とする著作物管理システム。

【0128】

(実施態様 1 6) 所定の作者により作成された原データを処理する情報処理方法であって、上記原データを変更する際に、その変更に関する変更情報を記憶媒体に記憶する変更情報記憶処理と、上記変更情報が原本であることを保証するための変更保証情報を作成する変更保証情報作成処理とを行うことを特徴とする情報処理方法。

【 0 1 2 9 】

(実施態様 1 7) 上記原データが原本であることを保証するための原データ保証情報を作成する原データ保証情報作成処理をさらに行うことを特徴とする実施態様 1 6 に記載の情報処理方法。

【 0 1 3 0 】

(実施態様 1 8) 上記原データと、上記原データ保証情報と、上記変更情報と、上記変更保証情報とを一体として管理する管理処理をさらに行うことを特徴とする実施態様 1 6 または 1 7 に記載の情報処理方法。

【 0 1 3 1 】

(実施態様 1 9) 上記原データと、上記原データ保証情報と、上記変更情報と、上記変更保証情報とを一体として送付する送付処理をさらに行うことを特徴とする実施態様 1 6 ～ 1 8 の何れか 1 項に記載の情報処理方法。

【 0 1 3 2 】

(実施態様 2 0) 所定の作者により作成された原データを処理する情報処理方法であって、上記原データが正当なものであることを確認する原データ確認処理と、上記原データの変更に係る変更情報が正当なものであることを確認する変更情報確認処理と、上記原データと上記変更情報が正当であることが確認された場合に、上記変更情報に応じて上記原データを変更する原データ変更処理とを行うことを特徴とする情報処理方法。

【 0 1 3 3 】

(実施態様 2 1) 上記原データ確認処理は、上記原データに対するデジタル署名を検証し、上記変更情報確認処理は、上記変更情報に対するデジタル署名を検証するようにしたことを特徴とする実施態様 2 0 に記載の情報処理方法。

【 0 1 3 4 】

(実施態様 22) 所定の作者により作成された原データを処理する情報処理方法であって、上記原データの変更に関する変更情報と、上記原データの変更履歴とを管理する管理処理を行うことを特徴とする情報処理方法。

【0135】

(実施態様 23) ネットワーク上で共有された電子データが正当なものであることと、上記電子データの変更に関する第 1 の変更情報が正当なものであることを確認する確認処理と、上記電子データと、上記第 1 の変更情報とが、上記確認処理により正当なものであることが確認された場合に、上記電子データを変更する電子データ変更処理と、上記電子データ変更処理により変更された電子データの変更に関する第 2 の変更情報と、上記第 2 の変更情報が正当なものであることを保証するための変更保証情報とを作成する情報作成処理と、上記情報作成処理により作成された第 2 の変更情報と、変更保証情報とを上記ネットワークに送信する送信処理とを行うことを特徴とする情報処理方法。

【0136】

(実施態様 24) 上記第 1 及び第 2 の変更情報と、上記原データの変更履歴を表す情報とのうち、少なくとも何れか一方を管理する変更履歴管理処理をさらに行うことを特徴とする実施態様 23 に記載の情報処理方法。

【0137】

(実施態様 25) 上記電子データ及び上記第 1 の変更情報のうち少なくとも何れか一方が正当でないということが上記確認処理により確認された場合に、その旨を通知する通知処理をさらに行うことを特徴とする実施態様 23 または 24 に記載の情報処理方法。

【0138】

(実施態様 26) 著作者が正当と認めたユーザが所有する情報処理装置に対して、上記著作者が所有する第 1 の情報処理装置から 1 次著作物を配布する 1 次著作物配布処理と、上記 1 次著作物配布処理により 1 次著作物が配布された情報処理装置により、上記著作者から認められた許諾範囲内で 1 次著作物を変更し、その変更内容を表す変更情報と、その変更情報が原本であることを保証するための第 1 の変更保証情報とを、上記第 1 の情報処理装置に送信する送信処理と

、上記変更情報と上記第 1 の変更保証情報との送信先である上記第 1 の情報処理装置により、上記送信された変更情報が正当なものであることを、上記第 1 の変更保証情報を用いて確認し、正当であることを確認した場合に、上記送信された変更情報が正当なものであることを保証するための第 2 の変更保証情報を上記変更情報に付加して送信元の情報処理装置に返信する返信処理とを行い、上記変更情報と、上記第 2 の変更保証情報とが返信された情報処理装置に対して、上記 1 次著作物を変更したものを 2 次著作物として使用することを許諾するようにしたことを特徴とする情報処理方法。

【0 1 3 9】

(実施態様 2 7) 所定の作者により作成された原データを変更する際に、その変更に関する変更情報を記憶媒体に記憶する変更情報記憶処理と、上記変更情報が原本であることを保証するための変更保証情報を作成する変更保証情報作成処理とをコンピュータに実行させることを特徴とするコンピュータプログラム。

【0 1 4 0】

(実施態様 2 8) 所定の作者により作成された原データが正当なものであることを確認する原データ確認処理と、上記原データの変更にに関する変更情報が正当なものであることを確認する変更情報確認処理と、上記原データと上記変更情報が正当であることが確認された場合に、上記変更情報に応じて上記原データを変更する原データ変更処理とをコンピュータに実行させることを特徴とするコンピュータプログラム。

【0 1 4 1】

(実施態様 2 9) 所定の作者により作成された原データの変更にに関する変更情報と、上記原データの変更履歴とを管理する管理処理をコンピュータに実行させることを特徴とするコンピュータプログラム。

【0 1 4 2】

(実施態様 3 0) ネットワーク上で共有された電子データが正当なものであることと、上記電子データの変更にに関する第 1 の変更情報が正当なものであることとを確認する確認処理と、上記電子データと、上記第 1 の変更情報とが、上記確認処理により正当なものであることが確認された場合に、上記電子データを変

更する電子データ変更処理と、上記電子データ変更処理により変更された電子データの変更に関する第2の変更情報と、上記第2の変更情報が正当なものであることを保証するための変更保証情報とを作成する情報作成処理と、上記情報作成処理により作成された第2の変更情報と、変更保証情報とを上記ネットワークに送信する送信処理とをコンピュータに実行させることを特徴とするコンピュータプログラム。

【0143】

(実施態様31) 著作者が正当と認めたユーザが所有する情報処理装置に対して、上記著作者が所有する第1の情報処理装置から1次著作物を配布する1次著作物配布処理と、上記1次著作物配布処理により1次著作物が配布された情報処理装置により、上記著作者から認められた許諾範囲内で1次著作物を変更し、その変更内容を表す変更情報と、その変更情報が原本であることを保証するための第1の変更保証情報とを、上記第1の情報処理装置に送信する送信処理と、上記変更情報と上記第1の変更保証情報との送信先である上記第1の情報処理装置により、上記送信された変更情報が正当なものであることを、上記第1の変更保証情報を用いて確認し、正当であることを確認した場合に、上記送信された変更情報が正当なものであることを保証するための第2の変更保証情報を上記変更情報に付加して送信元の情報処理装置に返信する返信処理とを行い、上記変更情報と、上記第2の変更保証情報とが返信された情報処理装置に対して、上記1次著作物を変更したものを2次著作物として使用することを許諾するようにしたことをコンピュータに実行させることを特徴とするコンピュータプログラム。

【0144】

(実施態様32) 上記実施態様27～31の何れか1項に記載のコンピュータプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【0145】

【発明の効果】

以上説明したように本発明によれば、所定の作者により作成された原データを変更する際に、その変更に関する変更情報を記憶媒体に記憶するとともに、上記

変更情報が原本であることを保証するための変更保証情報を作成するようにしたので、上記変更保証情報に基づいて上記原データの変更が正当なものであるか否かを判断し、正当なものである場合には上記変更情報により上記原データを変更することができるようになる。したがって、上記原データの原本性を保証しながら、上記原データの作者が認める正当な変更を行うことができ、上記原データの原本性と、データの最新性の両方を保証することができる。また、上記変更情報により、上記原データと、変更したデータとの関係を知ることができ、上記原データと、変更したデータとが適切な関係にあることを保証することができる。さらに、上記変更情報は、上記変更したデータそのものに比べてデータ量が少ないので、上記原データを変更するのに要する記憶容量を可及的に小さくすることができる。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施の形態を示し、記録媒体に記録される原画像、署名、及び履歴情報を示した概念図である。

【図 2】

本発明の第 1 の実施の形態を示し、電子署名を生成する際の処理を説明するフローチャートである。

【図 3】

本発明の第 1 の実施の形態を示し、電子署名を検証する際の処理を説明するフローチャートである。

【図 4】

本発明の第 1 の実施の形態を示し、情報処理装置の構成の一例を示したブロック図である。

【図 5】

本発明の第 2 の実施の形態を示し、記録媒体に記録される原画像、署名、及び履歴情報を示した概念図である。

【図 6】

本発明の第 2 の実施の形態を示し、履歴情報と電子署名とを処理ごとにまとめ

たリストの一例を示した図である。

【図 7】

本発明の第 3 の実施の形態を示し、電子データ管理システムの構成の一例を示したブロック図である。

【図 8】

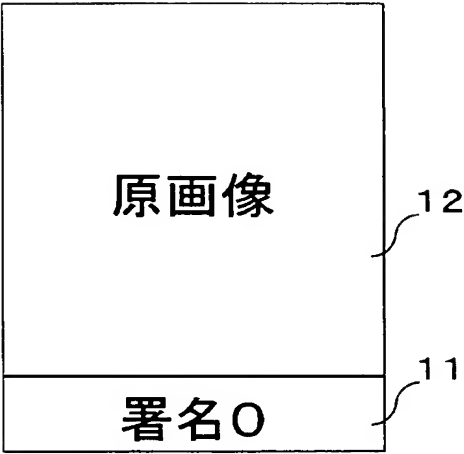
本発明の第 5 の実施の形態を示し、著作物管理システムで行われる処理を説明するフローチャートである。

【符号の説明】

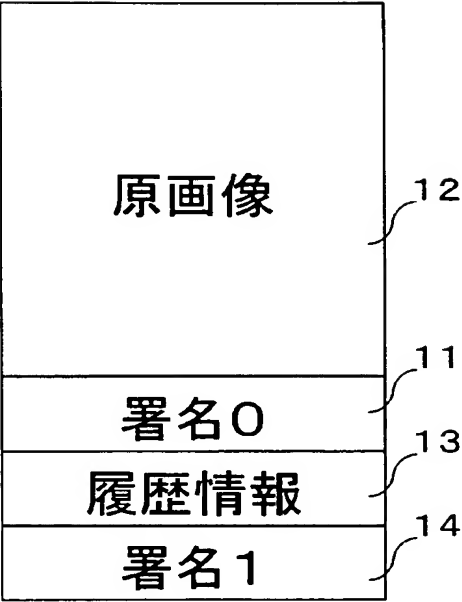
- 1 1、1 4、1 6 電子署名
- 1 2 原画像
- 1 3、1 5 履歴情報
- 3 0 1 情報処理装置
- 6 0 1 サーバ
- 6 0 2 電子文書
- 6 0 3～6 0 5 ユーザ

【書類名】 図面

【図 1】

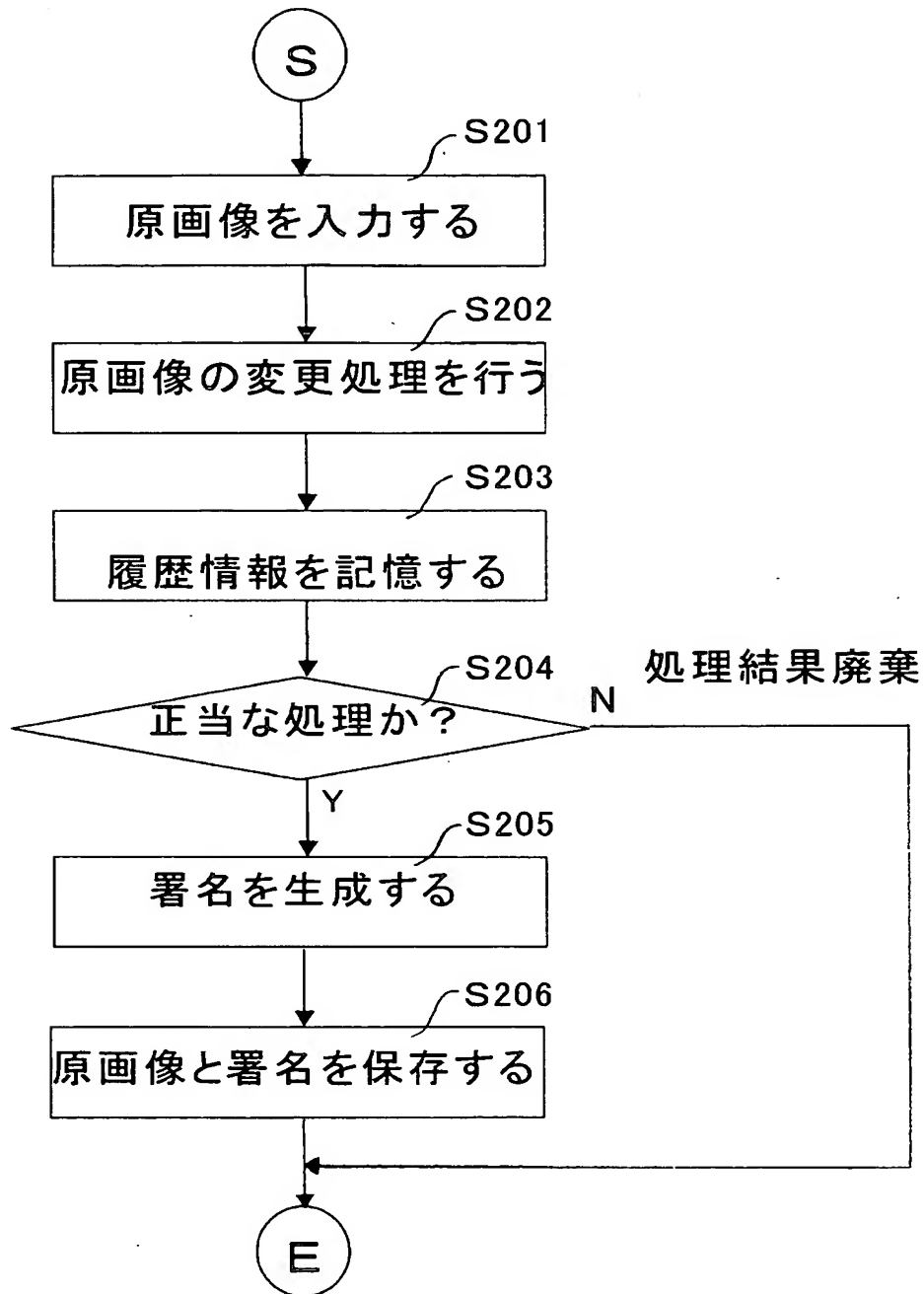


(a)

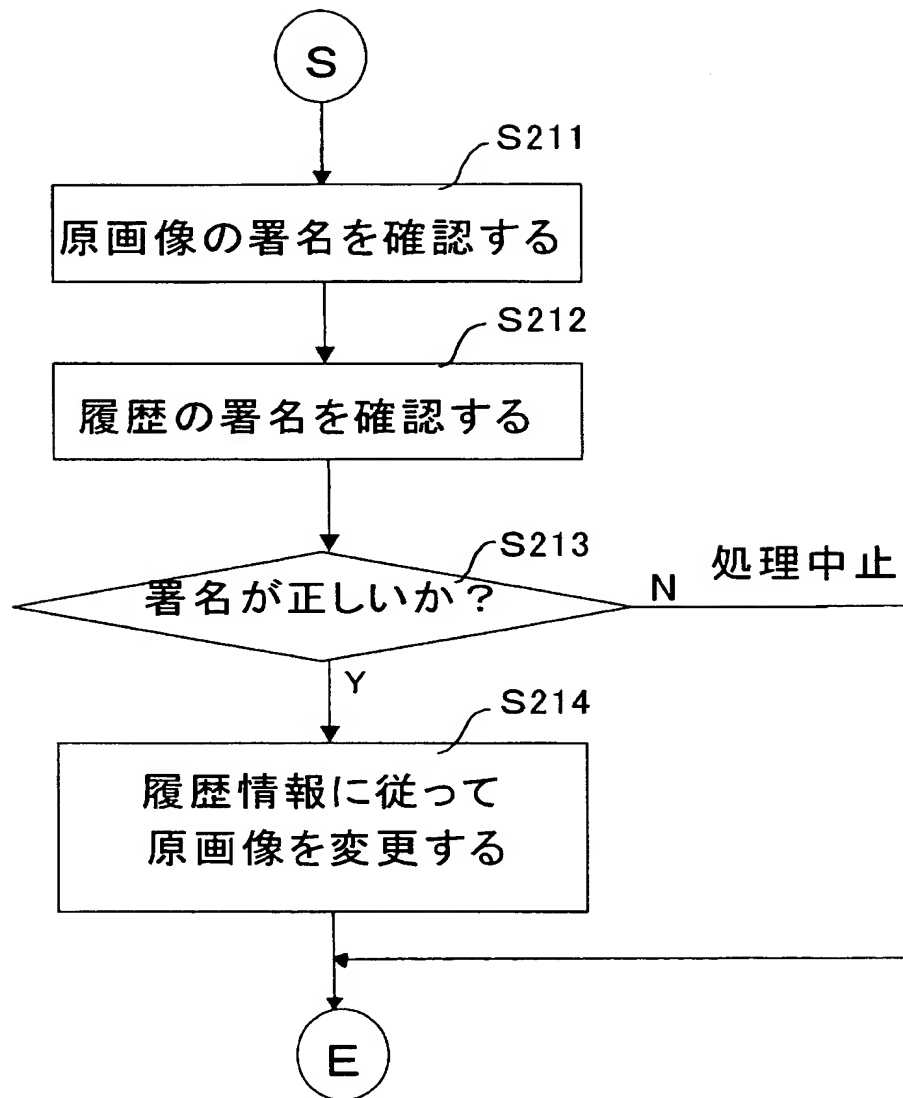


(b)

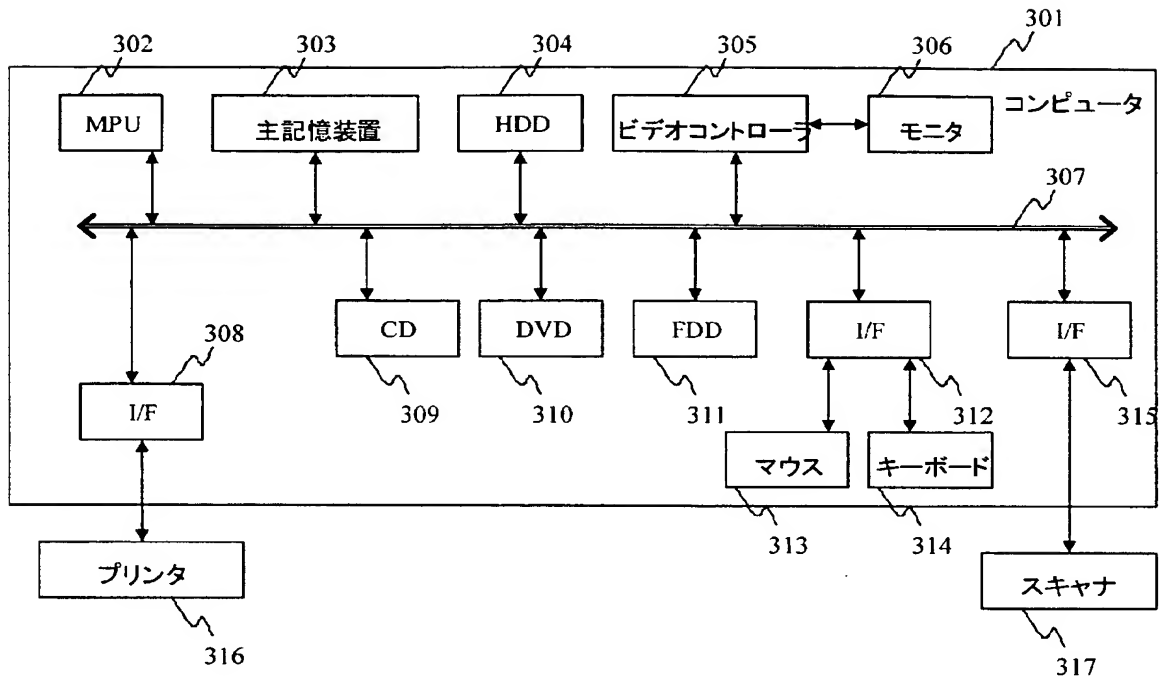
【図 2】



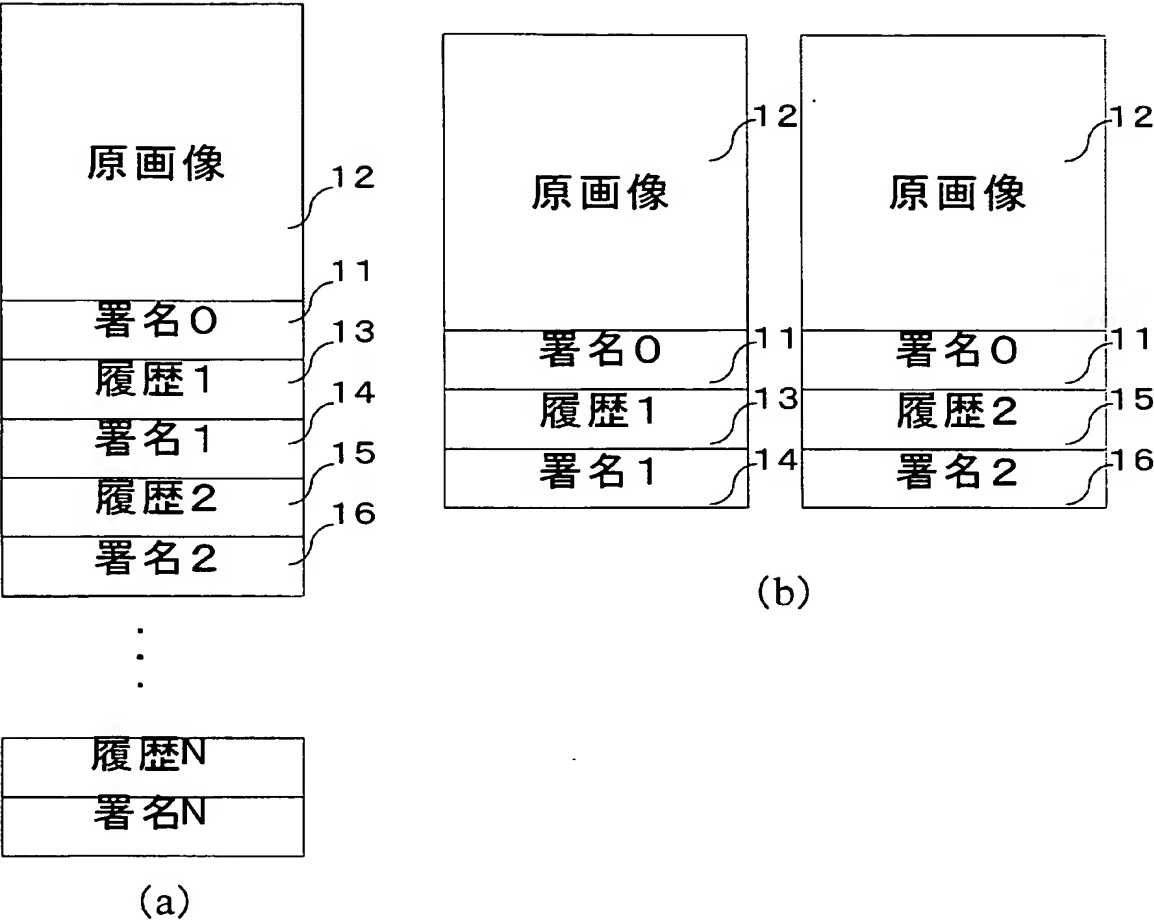
【図 3】



【図 4】



【図 5】

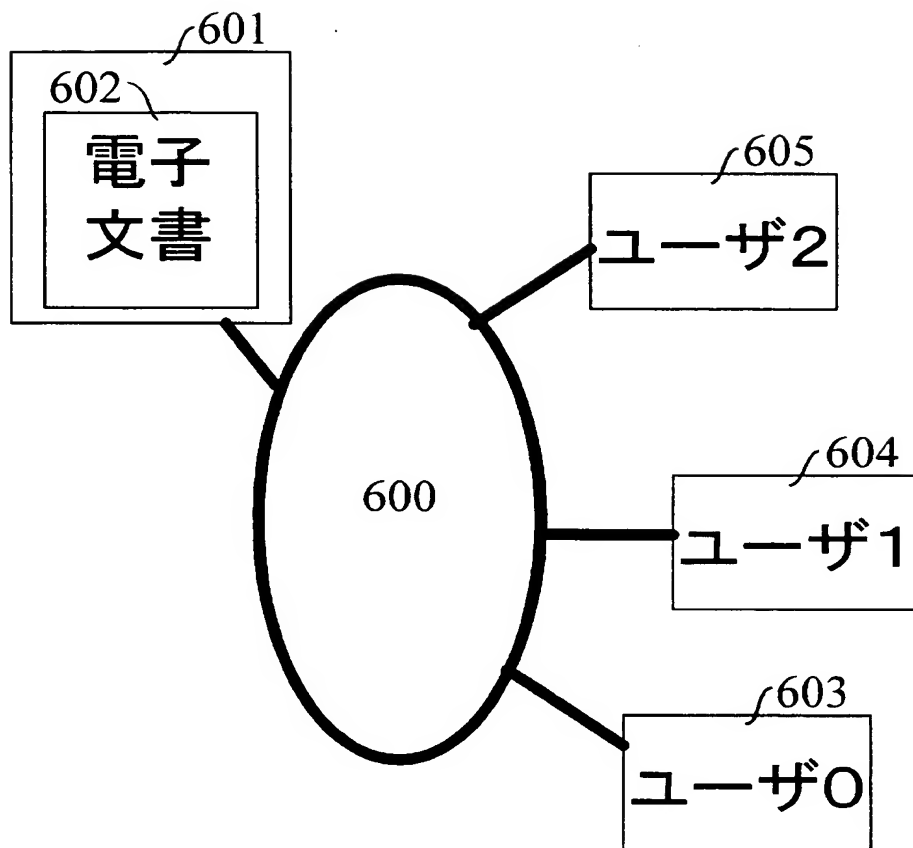


【図 6】

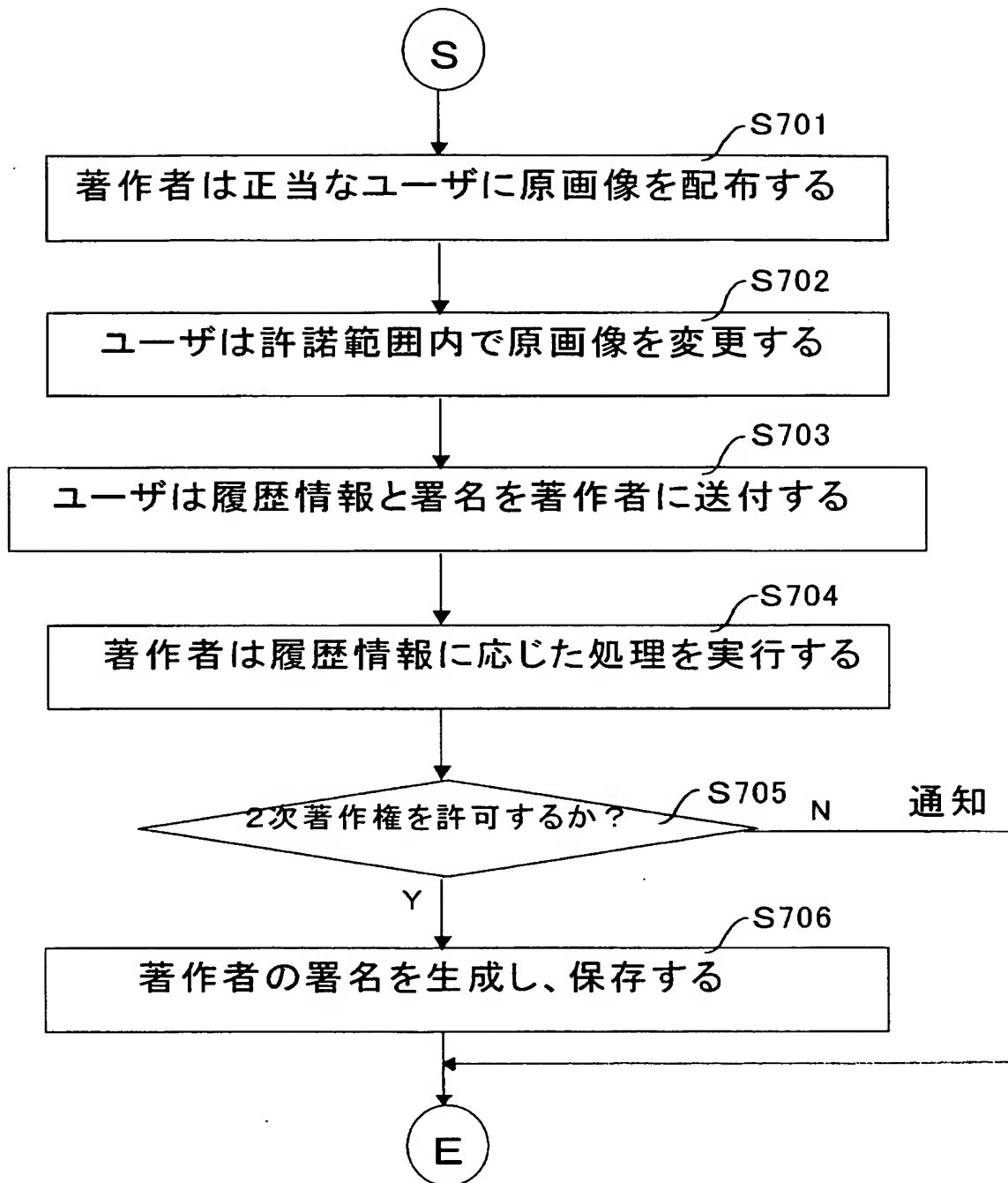
60

履歴情報	電子署名	用途
履歴 1	署名 1	輝度変換
履歴 2	署名 2	切り取り
・ ・ ・	・ ・ ・	・ ・ ・

【図 7】



【図 8】



【書類名】 要約書

【要約】

【課題】 データの原本性を保証しながら、上記データの作者が認める正当な変更を行えるようにする。

【解決手段】 所定の作者により作成された原画像 1 2 を変更する際に、その変更に関する履歴情報 1 3 と、履歴情報 1 3 が原本であることを保証するための第 2 の署名（署名 1） 1 4 とを作成することにより、上記作者や第三者が、上記変更が正当なものであるか否かを上記変更保証情報により判断することが可能になるようにする。これにより、原画像 1 2 の原本性を保証しながら、原画像 1 2 の作者が認める正当な変更を行えるようになる。

【選択図】 図 1

特願 2 0 0 2 - 3 3 2 5 7 7

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 1 0 0 7]

1. 変更年月日
[変更理由]

1 9 9 0 年 8 月 3 0 日
新規登録

住 所
氏 名

東京都大田区下丸子3丁目30番2号
キヤノン株式会社